(54) Title: SECURE SMART-ID PALMTOP DOCKING MODULE

(57) Abstract: The present invention describes an expan-
sion module for a handheld computer which allows the hand-
held computer (100) and expansion module (200) to func-
tion together as a secure security-ID terminal that accepts IC
based ID-cards (Smart Card) and IC based "dog-tags" and
presents the information to security personnel to validate the
card holders authority to enter into a secure area. The present
invention utilizes photo-ID and biometric data stored on the
IC based ID-card (Smart Card) and IC based "dog-tag" to
validate that the person presenting the credentials is in fact
the person authorized to be presenting them. The resultant
mobile secure security-ID terminal meets the advanced secu-
rity requirements of military and non-military security sites
worldwide. By disconnecting the handheld computer from
the expansion module, the handheld computer is restored to
conventional operation.

WO 02/071238 A1

Card Reader, and Settlement and Authentication System Using the Card Reader

5   <u>CROSS REFERENCE TO RELATED APPLICATION</u>

This application is based on Korea Patent Application No. 2001-28390 filed on May 23, 2001 in the Korean Intellectual Property Office, the content of which is incorporated herein by reference.

10   <u>BACKGROUND OF THE INVENTION</u>

(a) Field of the Invention

The present invention relates to a card reader. More specifically, the present invention relates to a card reader for reading IC (integrated chip) cards and interfacing with terminals including PCs (personal computers), and

15   a settlement and authentication system and method using the card reader.

(b) Description of the Related Art

Plastic credit cards as paying means for transactions have become generalized, and recently, IC cards have been developed as new paying means together with the development of semiconductors and information

20   communication technologies. Since commonly used plastic credit cards are easily duplicated, the IC cards will be gradually spread because of their hard-to-duplicate features.

A card reader for reading data stored in the IC card is required in

order to use the IC card. However, it costs a huge amount of money and time to disseminate the IC cards since the existing credit card readers provided all over the world need to be exchanged with new IC card readers, and software needed for reading the IC cards must be installed in the

5   corresponding devices.

Also, since electronic commerce has become much more available to people living all over the world through the Internet, and in particular, since electronic commerce is executed through wireless communication networks anytime, the IC cards are required for use as paying means anytime and

10   anywhere.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a card reader with easy portability for settling transactions through an IC card anytime.

15   It is another object of the present invention to provide a system and method for settling and authenticating transactions on a network using the card reader.

In one aspect of the present invention, a card reader for reading an IC card storing a pseudo number and providing information to an agency

20   terminal comprises: a reader for reading the pseudo number stored in the IC card; an input unit for inputting various types of information including a password for using the IC card; a processor for generating a user number on

processor for receiving a user number from the agency terminal, reading a user number from the database to determine whether they are matched, and when they are matched, finding a card number corresponding to the user number and executing a settlement process. It sequentially reads one of the user numbers stored in the database according to an established order, and compares the user number with a user number transmitted from the agency terminal.

In still another aspect of the present invention, a settlement method by a settlement system including a database for storing card numbers available by buyers, and a plurality of user numbers for each card number, the settlement system connected through a network to an agency terminal for transmitting user numbers provided by a card reader, comprises: searching the database and finding a corresponding card number when receiving an ID number and a user number from the agency terminal; determining whether to allow a transaction on the card number; and notifying the agency terminal of the transaction allowance when a transaction allowance on the card number is determined; and finding a card number that corresponds to the user number when the user number transmitted from the agency terminal is matched with the user number that corresponds to the currently using order.

The agency terminal transmits the user number provided by the card reader to the settlement system, and the card reader generates a user

4

number on the basis of the pseudo number encrypted from the IC card and the password input by the user, and provides the user number to the agency terminal.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate an embodiment of the invention, and, together with the description, serve to explain the principles of the invention:

FIG. 1 shows a block diagram of a card reader according to a preferred embodiment of the present invention;

FIG. 2 shows a state in which an IC card is inserted into a card reader according to a preferred embodiment of the present invention;

FIG. 3 shows a block diagram of a settlement and authentication system in cooperation with the card reader of FIG. 1; and

FIG. 4 shows a flowchart of a settlement method using the card reader according to a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following detailed description, only the preferred embodiment of the invention has been shown and described, simply by way of illustration

of the best mode contemplated by the inventor(s) of carrying out the invention. As will be realized, the invention is capable of modification in various obvious respects, all without departing from the invention. Accordingly, the drawings and description are to be regarded as illustrative in nature, and not restrictive.

FIG. 1 shows a configuration of a card reader according to a preferred embodiment of the present invention.

As shown, the card reader 10 comprises: a reader 11 for reading an IC card 20; an input unit 12 including a plurality of keys for inputting data including a password; a processor 13 for generating a settlement number (referred to as a "user number" hereinafter) on the basis of a password input through the input unit 12, and information read by the IC card 20; a data port 14 for transmitting and receiving data to/from an agency terminal 30 including a PC; a display 15 for displaying transmitted and received data; and an EEPROM (electrically erasable and programmable read only memory) 16.

The IC card 20 stores encrypted data for generating user numbers, and comprises a ROM that includes a COS (chip operating system) having an encryption function such as a CPU (central processing unit), an EEPROM, and a DES. The data stored in the IC card 20 comprises random numbers, a card password for generating a user number, and data of functions of an algorithm for generating the user number according to the preferred

6

embodiment of the present invention.

The data port 14 of the card reader 10 is connected to a PC or an agency terminal 30 for accessing a wireless communication terminal on the network, and it transmits and receives data. In particular, the data port 14 transmits the user number generated by the processor 13 to the connected agency terminal 30 so that the user number may be used as a settlement number when the agency terminal 30 executes transactions on the network. The data port 14 transmits and receives data to/from the agency terminal 30 through various interfacing methods including a USB (universal serial bus), Bluetooth technology, a serial connection, and a parallel connection.

The EEPROM 16 stores a password for generating a user number, and basic information on a processor's procedure.

The processor 13 decrypts the IC card's data read and output by the reader 11, and when a password is input from the input unit 12, the processor 13 generates a user number on the basis of the decrypted data and the input password. Referring to FIG. 1, the processor 13 comprises a password determination unit 131 for checking the password input from the input unit 12, and a number generator 132 for generating a user number on the basis of the data read by the IC card 20 and the input password.

For example, the processor 13 sums the data read and decrypted from the IC card 20, that is, a card password and a password input through the input unit 12 into a single number through a setting equation (e.g., a

length of summation of digits of the card password and digits of a personal password), and applies the summed value to the function of the algorithm to generate a user number (e.g., 16 digits).

The processor 13 may determine a matching state of the password input through the input unit 12, and then generate a user number as described above. For example, when the password input through the input unit 12 is matched with the password stored in the EEPROM 16, the processor 13 generates a user number on the basis of the input password and the decrypted card password. The processor 13 may execute a decryption process on the data read from the IC card 20 using the input password as a decryption key. In another way, the processor 13 stores a password for decryption at the initial operation stage in the EEPROM 16, and compares a subsequently input number with the stored password, and when they are matched, the processor 13 may decrypt the IC card 20.

The processor 13 provides the user number generated in the above manner to the agency terminal 30 connected through the data port 14, and when the agency terminal 30 is not connected through the data port 14, the processor 13 stores the generated user number in the EEPROM 16. When a number request signal is input from the agency terminal 30 through the data port 14, the processor 13 provides the stored user number to the agency terminal 30 through the data port 14.

In this instance, the generated user number is used once. For

example, a plurality of pseudo numbers may be stored in the IC card 20, and each time a password is input through the input unit 12, the reader 11 of the card reader 10 selects one of the pseudo numbers stored in the IC card 20 in use order, reads it, and decrypts it to generate a one-use number as described above. Also, one pseudo number may be stored in the IC card 20, and a plurality of user number generation rules may be stored in the EEPROM 16, and in this case, each time a password is input through the input unit 12, the processor 13 of the card reader 10 applies the pseudo number read and decrypted from the IC card 20 and the input password to a generation rule that corresponds to a currently used order according to a use order from among the user number generation rules to thereby generate a one-use number. That is, when the number read and decrypted from the IC card is matched with the input password, different user numbers may be generated by using different user number generation rules. In addition, the present invention is not restricted to the above-noted methods, but may further generate one-use user numbers by various methods.

FIG. 2 shows an external configuration of the card reader and a state of inserting an IC card into the card reader. As shown, the card reader is realized in a portable and small manner so that the user may connect the card reader to the agency terminal for settlement and authenticated anytime and anywhere. The portable card reader may be formed as an "electronic purse" but it is not restricted to this pattern.

The agency terminal 30 connected to the card reader and receiving the user number represents a communication device for executing electronic transactions through network media, such as a PC, a wireless communication terminal, and an Internet TV. As shown in FIG. 1, the agency

5   terminal 30 comprises an interface 31 for transmitting and receiving data to/from the data port 14 of the card reader 10, and in particular, software for executing transactions in cooperation with the card reader 10, that is, a processor 32, and a communication unit 33 for a network access. In addition, the agency terminal may comprise an input unit, a display, and a memory. In

10   this instance, the communication unit 33 comprises means that enable access through a network to transmit and receive data, such as a web browser for accessing the Internet, and a wireless transmitting and receiving unit of a wireless communication terminal.

The processor 32 provides the user number input from the card

15   reader 10 through the interface 31 to the settlement and authentication system connected on the network, so that the products (including all kinds of goods) bought by the user are automatically settled or authenticated when the user does not additionally input a user number.

FIG. 3 shows a settlement and authentication system in cooperation

20   with the card reader and the agency terminal as configured above. As shown, the settlement and authentication system 50 (Here, a settlement system is described as an example, and the system may be applied to user

authentication without being restricted to this.) is connected to an agency terminal 30 and an authentication system 60 for settlement and authentication through a network (including wire and wireless networks).

The settlement system, that is, the settlement system 50 may be managed by a VAN service provider, and the settlement system 50 comprises: a member database 51 for storing various categories of information for providing a settlement service using an IC card 20; an issue information database 52; a settlement database 53; a member manager 54 for providing a settlement service to users registered as members on the basis of information stored in the databases 51, 52, and 53; a number issuer 55; a settlement processor 56; and an information transmitting and receiving unit 57.

The member database 51 stores information on the users who are registered as members who may receive the settlement service using the IC card 20. For example, for each identification code, the member database 51 stores a name, a settlement password, unique card numbers of various cards of the user (e.g., credit cards and department store cards), a residence registration number, contact points (including email addresses, a postal address, a mobile phone number, and a wire phone number), and user information such as a place of residence.

The issue information database 52 stores a plurality of user numbers for providing use allowances corresponding to various card numbers of the

users for each identification number assigned to the IC card, and the user numbers corresponding to each card number are sequentially used according to a use order for each transaction. In addition, in the case of generating a card number through a rule, the issue information database 52 may store one user number (or at least one user number) for each card number.

The settlement database 53 stores settled cards for each user who requests settlements, and corresponding settlement history.

The member manager 54 interfaces with other systems (an agency terminal and an authentication system) that access through the network 40, and in particular, it processes membership registration that enables receiving of the settlement service and member log-in at the time of an access.

The number issuer 55 provides a user number that represents a use allowance for each card of a user registered as a member.

When receiving a user number from the agency terminal 30, the settlement processor 56 determines whether the received user number is matched with the user number (the user number to be currently used) stored in the issue information database 52, and requests a transaction allowance from the authentication system 60 according to determination results. When the settlement system 50 is a card company that issues the cards, the settlement processor 56 processes a transaction allowance on the basis of information stored in an additional card information database (not illustrated)

that stores transaction limits and credits for each card member without operating the authentication system 60.

The information transmitting and receiving unit 57 transmits and receives information to/from the agency terminal 30, and in particular, it

5   transmits transaction allowance results to the agency terminal 30 through the network 40.

In the case the settlement system concurrently executes an authentication-related function according to the disclosure of the present invention, the database of the settlement system may be modified so as to

10   execute user authentication on the basis of the above-described technique.

In the following, an operation of the card reader and a settlement operation for transactions through card reading will be described in detail on the basis of the above configuration.

FIG. 4 shows a flowchart of a settlement method according to the

15   preferred embodiment of the present invention.

When a user registered as a member who may receive a settlement service of the settlement system inserts an IC card 20 into the reader 11 of the card reader 10 for a settlement (or an authentication) process, an initial settlement screen for inputting a password is displayed on the display 15 of

20   the card reader 10. When the user inputs a password of the IC card 20 so as to execute a settlement, the password is input to the processor 13 through the input unit 12 in steps S60 and S61.

When the password is input, the processor 13 outputs an instruction to the reader 11 to read the data stored in the inserted IC card 20, and the reader 11 accordingly reads the data stored in the IC card 20 and outputs them to the processor 13 in step S62. In this instance, the data read from the IC card 20 are encrypted data.

The processor 13 decrypts the data read from the IC card 20, and applies the decrypted data and the password input by the user to a setting equation for generating a user number to thereby generate a user number. For example, the processor 13 sums the data read and decrypted from the IC card 20, that is, the card password, and a password input through the input unit 12 into a single number (e.g., a length of summed digits of digits of the card password and digits of a personal password) through a setting equation, and applies to summed value to a function of an algorithm to generate a user number (e.g., 16 digits) in steps S63 and S64. In this instance, the generated user number is used once, and when used once, it is automatically discarded. Since its generation method has been previously described, no further description will be provided.

When the user number is generated, the processor 13 selectively transmits the generated user number to the agency terminal 30 depending on whether the agency terminal is connected to the data port 14.

For example, when a user or a seller connects the card reader 10 to the agency terminal 30 such as a PC, connects the agency terminal 30 to the

settlement system 50 through the network 40, and requests a settlement from the settlement system 50, the settlement system 50 requests a user number from the agency terminal 30. Under this state, when the user number generated on the basis of the number read from the IC card of the user and the password input by the user is input through the data port 14 of the card reader 10, the agency terminal 30 automatically transmits the input user number together with a transaction history to the settlement system 50 to request a final settlement in step S65.

In addition, the processor 13 of the card reader 10 displays the generated user number on the display 15 so that the user may settle or be authenticated using this number when the agency terminal 30 is not connected to the card reader 10.

Namely, when the user makes a purchase at a shopping mall site on the network, the user may use the user's terminal (an agency terminal) to transmit the user number displayed on the card reader to the settlement system. Also, when the user buys goods at a general card member store, the user may provide the user number displayed on the card reader to a shopkeeper of the member store so that the shopkeeper may use the shopkeeper's terminal (an agency terminal) to transmit the user number to the settlement system.

When receiving the user number generated from the card reader 10 in the above-noted various methods, the agency terminal 30 transmits a

15

transaction history and items related to the user number to the settlement

system through the network 40, and in this instance, the data transmitted to

the settlement system 50 include an identification number assigned to the IC

card.

5   The settlement processor 56 of the settlement system 50 receives

the items related to the user number and the transaction history from the

agency terminal 30, searches for the issue information database 52 on the

basis of the received identification number, finds one user number that

corresponds to the currently processed order according to the use order from

10   among a plurality of user numbers assigned to the card of the user who

requests a settlement, determines whether the one user number is matched

with the user number transmitted from the agency terminal, and

authenticates a settlement according to matching status of the two user

numbers in steps S66 and S67.

15   When the two user numbers are matched, the settlement system 56

transmits the card number of the card company matched with the user

number, and the transaction history, to the authentication system 60 that is

managed by the card company to request a transaction authentication in

step S68. In the case the company that provides the service according to the

20   embodiment of the present invention issues the cards, information on the

transaction limit and the current available service status may be stored in the

settlement system for each card. In this instance, the settlement processor

may determine settlement allowing states without asking for a transaction allowance of the card company, and hence, the step of requesting a transaction allowance may be omitted.

When a transaction allowance is sent from the authentication system

5   60 or it is determined by the settlement processor, the settlement system transmits transaction allowance results together with the corresponding user number (and a member ID used for an accessing stage when attempting to do electronic commerce) to the agency terminal 30 in steps S69 and S70. When a transaction rejection is sent from the authentication system 60 or a

10 transaction allowance is rejected by the settlement processor, the settlement system transmits a transaction-rejected message together with the corresponding user number (or a member ID) to the agency terminal 30. In this instance, the settlement system notifies the user that the transaction is rejected through the number, asks the user to input the accurate number,

15 and when the allowance errors are repeated a predetermined number of times, when an accurate user number is input within a predetermined time but a corresponding allowance is not received, or when the predetermined time for inputting a number for receiving an allowance has expired, the settlement system immediately stops the settlement process and wirelessly

20 notifies the card user of the stopped status so as to instantly interrupt an illegal use.

When notifying of an allowance result corresponding to a settlement

17

request, the settlement processor 56 of the settlement system 50 records

that a transaction is executed in correspondence to the settled card when the

allowance is provided, or with no relation to the allowance result, and the

settlement processor 56 uses a subsequent user number according to an

5   established order in the subsequent transaction.

As described, the card reader for executing a settlement and

authentication process in cooperation with the settlement and authentication

system on the network basis may check the balance.

Also, the card reader may be used as means for storing

10   configuration data (e.g., PC information such as email accounts that the user

is required to memorize) so as to build its environments in any type of PC,

and in addition, the card reader may store a code table (a password table)

used for executing a PC banking service or a telebanking service managed

by banks.

15   The present invention provides a card reader for providing easy

portability, and for enabling the user to execute electronic transactions and

settle them using an IC card anytime and anywhere.

Further, in the next settlement and authentication transaction, the

present invention allows use of a different user number to thereby protect the

20   IC card user when the user number is stolen.

While this invention has been described in connection with what is

presently considered to be the most practical and preferred embodiment, it is

to be understood that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

5

WHAT IS CLAIMED IS:

1. A card reader for reading an IC card storing a pseudo number and providing information to an agency terminal, comprising:

a reader for reading the pseudo number stored in the IC card;

an input unit for inputting various types of information including a password for using the IC card;

a processor for generating a user number on the basis of the password input through the input unit and the pseudo number output from the reader; and

a data port for selectively transmitting the generated user number to the agency number.

2. The card reader of claim 1, wherein the user number is used once.

3. The card reader of claim 1, further comprising a display for displaying the user number generated by the processor.

4. The card reader of claim 1, wherein the card reader further comprises a memory for storing a password for using the IC card, and the processor generates a user number on the basis of the password output by the input unit and the pseudo number read by the IC card when the password output by the input unit is matched with the password stored in the memory.

5. The card reader of claim 1, wherein the pseudo number read by

the IC card is encrypted, and the processor decrypts the read pseudo number, and combines the decrypted pseudo number with the subsequently input password to generate a user number.

6. The card reader of claim 1, wherein the agency terminal is a communication device for providing the user number transmitted through the data port to a settlement and authentication system through a network so as to settle and authenticate the IC card user.

7. A settlement system connected through a network to an agency terminal for transmitting a user number provided by a card reader, comprising:

a database for storing a plurality of user numbers for each card number usable by a buyer; and

a processor for receiving a user number from the agency terminal, and reading a user number from the database to determine whether they are matched, and when they are matched, finding a card number corresponding to the user number and executing a settlement process, and the processor sequentially reading one of the user numbers stored in the database according to an established order and comparing the user number with a user number transmitted from the agency terminal.

8. The settlement system of claim 7, wherein the agency terminal transmits the user number provided by the card reader to the settlement system, and the card reader generates a user number on the basis of the

pseudo number encrypted from the IC card and the password input by the user, and provides the user number to the agency terminal.

9. A settlement method by a settlement system including a database for storing card numbers available by buyers, and a plurality of user numbers for each card number, the settlement system connected through a network to an agency terminal for transmitting user numbers provided by a card reader, comprising:

searching the database and finding a corresponding card number when receiving an ID number and a user number from the agency terminal;
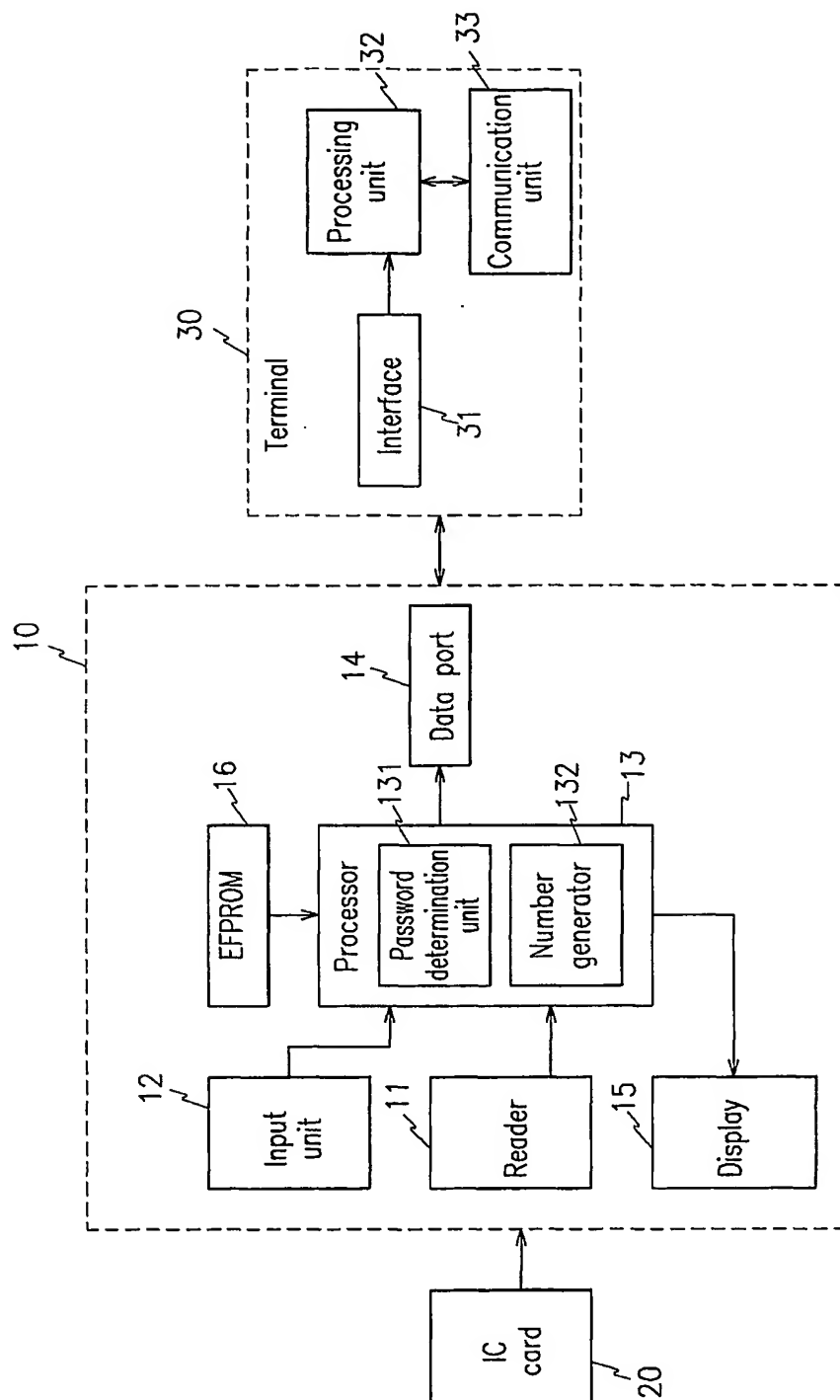
determining whether to allow a transaction on the card number; and

notifying the agency terminal of the transaction allowance when a transaction allowance on the card number is determined; and finding a card number that corresponds to the user number when the user number transmitted from the agency terminal is matched with the user number that corresponds to the currently used order.

10. The settlement method of claim 9, wherein the agency terminal transmits the user number provided by the card reader to the settlement system, and the card reader generates a user.number on the basis of the pseudo number encrypted from the IC card and the password input by the user, and provides the user number to the agency terminal.
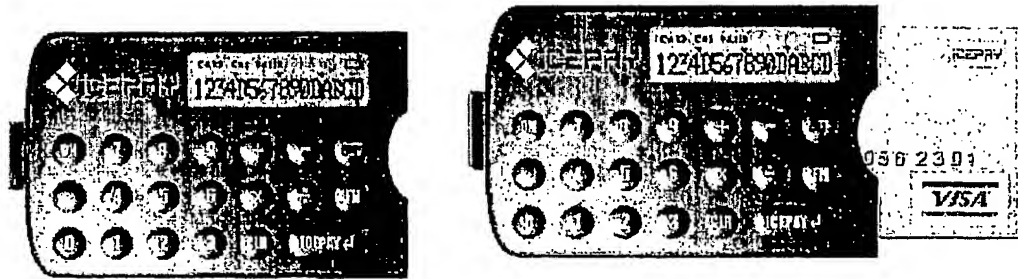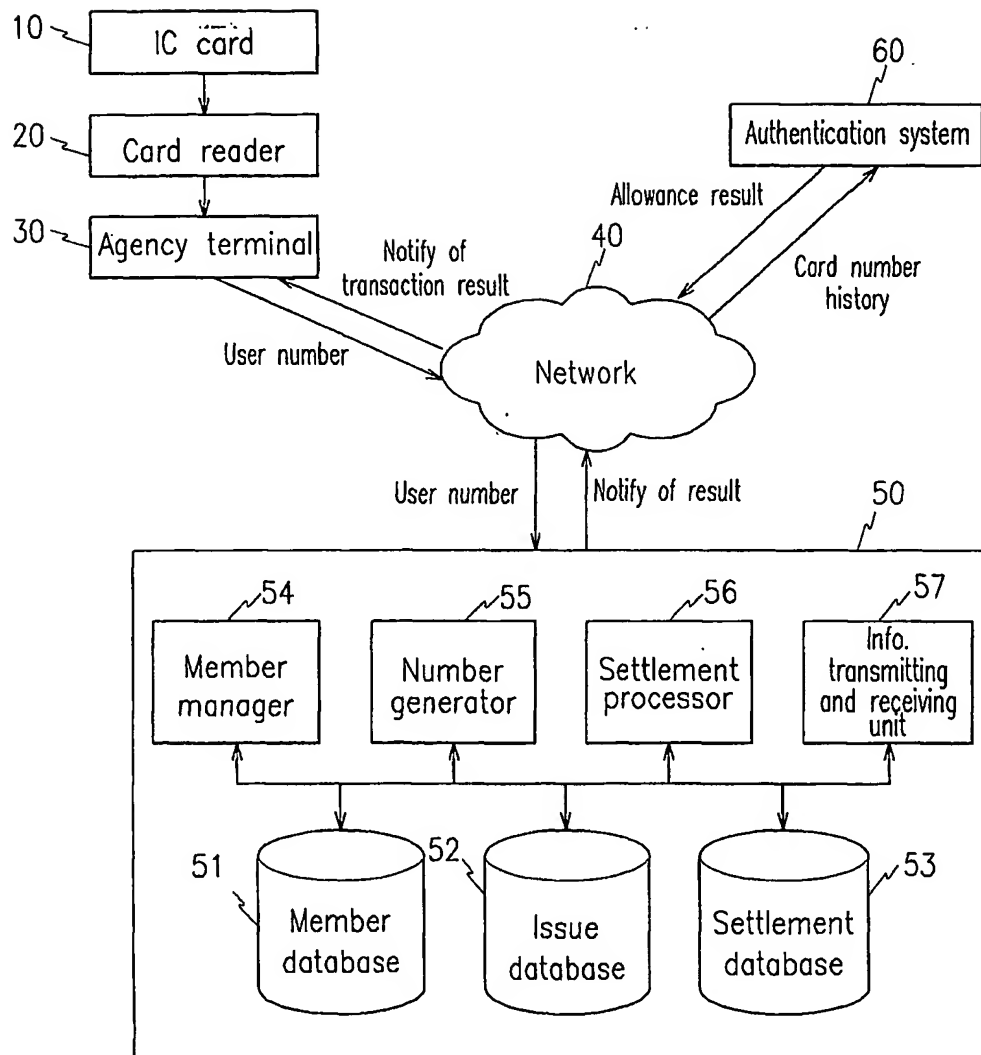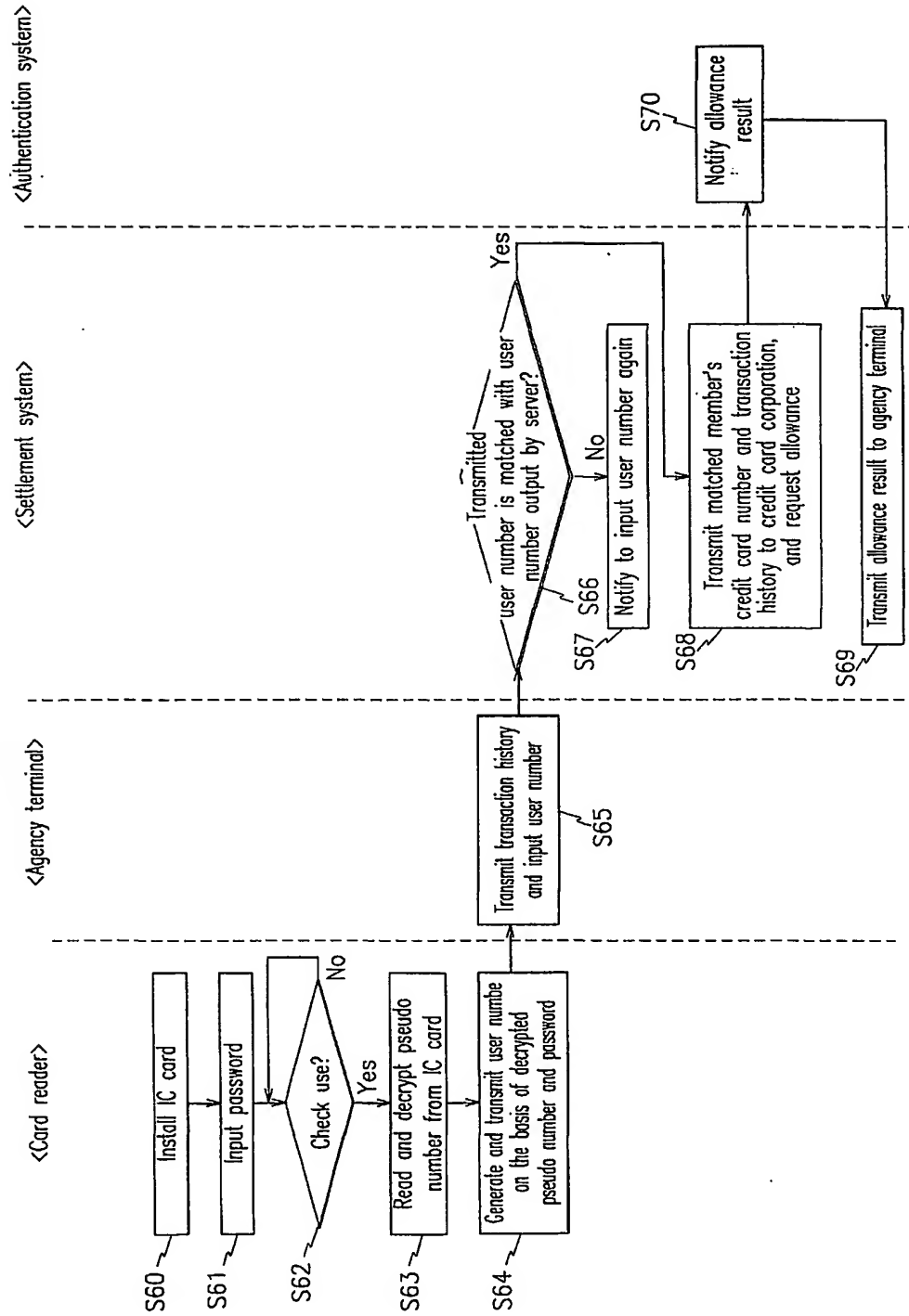
FIG.1

FIG.2

FIG.3

4/4

FIG.4

<Card reader>   <Agency terminal>   <Settlement system>   <Authentication system>

S60 — Install IC card

S61 — Input password

S62 — Check use?
No / Yes

S63 — Read and decrypt pseudo number from IC card

S64 — Generate and transmit user numbe on the basis of decrypted pseudo number and password

S65 — Transmit transaction history and input user number

Transmitted user number is matched with user number output by server?
No / Yes

S66 / S67 — Notify to input user number again

S68 — Transmit matched member's credit card number and transaction history to credit card corporation, and request allowance

S69 — Transmit allowance result to agency terminal

S70 — Notify allowance result

INTERNATIONAL SEARCH REPORT

A.	CLASSIFICATION OF SUBJECT MATTER

IPC7 G06K 17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B.	FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

(IPC7) G06K, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

KR,JP: IPC as above

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search terms used)
KIPONET

C.	DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR2000-6590A (LEE, Jong in) 7 February 2000 See the abstract and figures	1-10
A	KR1999-213188B1 (Samsung Electronics co. , LTD.) 2 August 1999 See the abstract and figures	1-10
A	US6000607A (Hitachi, LTD.) 14 December 1999 See the abstract and figures	1-10
A	JP9-259239A (Toshiba Corp.) 3 October 1997 See the abstract and figures	1-10
A	JP2000-207614A (Hitachi LTD. , Hitachi Media Electronics Co.LTD.) 28 July 2000 See the abstract and figures	1-10

☐ Further documents are listed in the continuation of Box C.   ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevence	
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)	"Y" document of particular relevence; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 SEPTEMBER 2002 (18.09.2002)	18 SEPTEMBER 2002 (18.09.2002)

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea	JEON, Il Yong
Facsimile No. 82-42-472-7140	Telephone No. 82-42-481-5981

Form PCT/ISA/210 (second sheet) (July 1998)